Amendments to the Claims:

This listing will replace all prior versions, and listings, of the claims in the application.

Please cancel Claims 3-6, 8, 9, 14, 15 and 27-30, without prejudice or disclaimer.

Listing of Claims:

1. (currently amended) An authentication method wherein:

a user owns an electronic value including encrypted value authentication information (F(VPW)) wherein ~~said~~ authentication information (VPW) corresponding to said electronic value specified by said user is encoded by a first irreversible calculation process (F),

in a process for authenticating said user as the right owner of said electronic value, an authentication side generates a random number (R) and transmits it to said user side,

[[a]] said user side generates value authentication information (F(VPW')) from authentication information (VPW) corresponding to [[an]] said electronic value input by user, further generates authentication information (G(R,F(VPW'))) wherein said random number (R) and said value authentication information (F(VPW')) are concatenated and encoded by a second irreversible calculation process (G) and transmits said electronic value and said authentication information (G(R,F(VPW'))) to said authentication side,

said authentication side decrypts code of said received electronic value, extracts said value authentication information (F(VPW)) from said electronic value, generates authentication information (G(R,F(VPW))) wherein said random number (R) and said value authentication information (F(VPW)) are concatenated and encoded by said second irreversible calculation

process (G), collates said received authentication information (G(R,F(VPW'))) with said generated authentication information (G(R,F(VPW))), verifies that they are identical, and authenticates user.

2. (currently amended) The authentication method of claim 1 wherein:

a decryption key of an encrypted part of said electronic value is generated from data (H(F(VPW))) wherein said value authentication information (F(VPW)) is encoded by a third irreversible calculation process (H) and a master key,

in said process for authenticating said user as the rightful owner of said electronic value, said user side further generates data (H(F(VPW'))) wherein said value authentication information (F(VPW')) is encoded by said third irreversible calculation process (H), transmits data (H(F(VPW'))) with said electronic value and said authentication information (G(R,F(VPW'))) to said authentication side,

said authentication side generates **[[a]]** said decryption key from received data (H(F(VPW'))) and master key, and decrypts code of received electronic value.

Claims 3-6 – (canceled)

7. (currently amended) A mobile terminal wherein:

comprising storage means storing an electronic value, generating value authentication information (F(VPW')) wherein value authentication information (VPW') corresponding to said electronic value input by a user is encoded by a first irreversible calculation process (F), further generating a second random number (R2), further encoding by an irreversible calculation process

(F) ~~on data~~ wherein said value authentication information (F(VPW')) and a first random number (R1) received from an authentication apparatus are concatenated, generating said authentication information (G(R1,F(VPW'))) by a second irreversible calculation process (G), and transmitting said electronic value, authentication information (G(R1,F(VPW'))) and said second random number (R2) to said authentication apparatus, thereby authenticating said user to be the rightful owner of said electronic value.

Claims 8 and 9 – (canceled)

10. (currently amended) The mobile terminal of ~~any one of claims~~ claim 7 ~~to 9~~ wherein:

a decryption key of encrypted part of said electronic value is generated from data (H(F(VPW))) wherein value authentication information (F(VPW)) is encoded by a fourth irreversible calculation process (H) and a master key, said mobile terminal generates data (H(F(VPW'))) wherein said value authentication information (F(VPW')) is encoded by said fourth irreversible calculation process (H) and transmits said electronic value, said authentication information (G(R,F(VPW'))) and said data (H(F(VPW'))))to said authentication apparatus, thereby authenticating said user to be the rightful owner of said electronic value.

11. (currently amended) The mobile terminal of ~~any one of claims~~ claim 7 ~~to 9~~ characterized in that:

said storage means stores a property which is attribute information set with respect to each electronic value ~~with said electronic value~~,

in authentication process with the use of said electronic value, an operation is executed based on said property.

12. (currently amended) The mobile terminal of ~~any one of claims~~ claim 7 ~~to 9~~ characterized in that:

said storage means stores a property which is attribute information set with respect to each electronic value ~~with said electronic value~~,

in authentication process with the use of said electronic value, an operation is executed based on user terminal control information received from said authentication information and said property.

13. (currently amended) An authentication apparatus characterized in:

generating a random number (R) and transmitting it to a mobile terminal, receiving authentication information (G(R,F(VPW'))) and an electronic value from said mobile terminal, decrypting code of an encrypted part of said electronic value, and validating said electronic value, further extracting value authentication information (F(VPW)) from said electronic value, wherein the function (F) is a first irreversible calculation process, generating authentication information (G(R,F(VPW))) wherein said value authentication information (F(VPW)) and said random number (R) are concatenated and encoded by [[an]] a second irreversible calculation process (G), and collating received authentication information (G(R,F(VPW'))) with generated authentication information (G(R,F(VPW))), verifying that they are identical, thereby authenticating a user.

Claims 14 and 15 – (canceled)

16. (currently amended) The authentication apparatus of ~~any one of claims~~ claim 13 ~~to 15~~ wherein:

a decryption ~~key of~~ for said encrypted part of said electronic value is generated from data (H(F(VPW))) wherein said value authentication information (F(VPW)) is encoded by a third irreversible calculation process (H) and a master key,

said authentication apparatus generates said decryption key from data (H(F(VPW'))) received from said mobile terminal and said master key, and decrypts code of received electronic value.

17. (currently amended) The authentication apparatus of ~~any one of claims~~ claim 13 ~~to 15~~, comprising a security module having a tamper-resistant function, characterized in that:

said security module decrypts the encrypted part of said electronic value, stores a negative list of electronic values, and verifies that said received electronic value is not listed in said negative list of electronic value at the point of validation of said received electronic value.

18. (original) The authentication apparatus of claim 17 wherein:

said security module communicates with a center and updates information stored in said security module.

19. (currently amended) The authentication apparatus of ~~any one of claims~~ claim 13 ~~to 15~~ wherein:

transmitting user terminal information to [[a]] said mobile terminal and controlling operation of said mobile terminal at the point of ~~authentication process~~ said authenticating step by said electronic value and executing operation of its own based on service terminal control information received from said mobile terminal.

20. (currently amended) An electronic value issuance server wherein:

extracting authentication information (VPW) corresponding to an electronic value specified by a user from electronic value issuance request received from said mobile terminal, generating value authentication information (F(VPW)) wherein authentication information (VPW) corresponding to said electronic value is encoded by [[said]] said first irreversible calculation process (F), generating a encryption key from data (H(F(VPW))) wherein said value authentication information (F(VPW)) is encoded by a third irreversible calculation process (H) and a master key, generating said electronic value with the use of said value authentication information (F(VPW)) and said generated encryption key, and transmitting [[it]] said electronic value to said mobile terminal.

21. (currently amended) An electronic value issuance server wherein:

extracting authentication information (F(VPW)) corresponding to an electronic value specified by user, wherein authentication information (VPW) is encoded by a first irreversible calculation process (F), from electronic value issuance request message received from a mobile terminal, generating an encryption key from data (H(F(VPW))) wherein said value authentication information (F(VPW)) is encoded by a second irreversible calculation process (H) and a master key, generating said electronic value with the use of said value authentication information

(F(VPW)) and said generated encryption key, and transmitting [[it]] said electronic value to mobile terminal.

22. (currently amended) The electronic value issuance server of either claim 20 or 21 wherein:

said electronic value includes electronic value disclosure information and security information,

said security information is data ~~wherein~~ including electronic value secret information, wherein said value authentication information (F(VPW)) and signature information are encrypted by said generated encryption key,

said signature information is a digital signature for data wherein said electronic value disclosure information, said electronic value secret information, and said value authentication information (F(VPW)) are concatenated.

23. (currently amended) The electronic value issuance server of either claim 20 or 21 wherein:

said electronic value includes electronic value disclosure information and security information,

said security information is data wherein electronic value secret information, said value authentication information (F(VPW)) and said signature information are encrypted by said generated encryption key,

said signature information is a result of a hash calculation for data wherein said electronic value disclosure information, said electronic value secret information, and said value authentication information (F(VPW)) are concatenated.

24. (currently amended) The electronic value issuance server of claim 22 wherein:

generating risk management information based on credit information of [[a]] said user and a result of risk evaluation on authentication information (F(VPW)) corresponding to said electronic value specified by said user and building said risk management information in said electronic value secret information.

25. (currently amended) An authentication system, comprised of a mobile terminal managed by a user, an authentication apparatus and an electronic value issuance server, wherein:

said mobile terminal stores an electronic value received from said electronic value issuance server,

said electronic value includes an encrypted value authentication information (F(VPW)) wherein authentication information (VPW) corresponding to said electronic value specified by said user is encoded by a first irreversible calculation process (F),

in a process for authenticating said user to be the rightful owner of said electronic value, said authentication apparatus generates a random number (R) and transmits [[it]] said random number to said mobile terminal,

said mobile terminal generates value authentication information (F(VPW')) from authentication information (VPW') corresponding to said electronic value specified by said user, further generates authentication information (G(R,F(VPW'))) wherein said value authentication

information (F(VPW')) and said random number (R) are concatenated and encoded by a second irreversible calculation process (G), and transmits said electronic value and said authentication information (G(R,F(VPW'))) to said authentication apparatus,

said authentication apparatus decrypts code of received electronic value, extracts value authentication information (F(VPW)) from said electronic value, generates authentication information (G(R,F(VPW))) wherein said value authentication information (F(VPW)) and said random number (R) are concatenated and encoded by said second irreversible calculation process (G), collates said received authentication information (G(R,F(VPW'))) with said generated authentication information (G(R,F(VPW))), verifies that they are identical, and authenticates said user.

26. (currently amended) The authentication system of claim 25 wherein:

said decryption key of an encrypted part of said electronic value is generated from data (H(F(VPW))) wherein said value authentication information (F(VPW)) is encoded by a third irreversible calculation process (H) and a master key,

in said process for authenticating said user as the right owner of said electronic value, said user side further generates data (H(F(VPW'))) wherein said value authentication information (F(VPW')) is encoded by a third irreversible calculation process (H), transmits data (H(F(VPW'))) with said electronic value and said authentication information (G(R,F(VPW'))) to authentication apparatus,

authentication apparatus generates a decryption key from received data (H(F(VPW'))) and master key, decrypts code of received electronic value.

Claims 27-30 – (canceled)

31. (currently amended) A lock apparatus wherein:

in issuance of an electronic key, an issuance function of said electronic key extracting authentication information (F(VPW)) corresponding to said electronic key specified by a user, wherein authentication information (VPW) is encoded by a first irreversible calculation process (F), from **[[an]]** said electronic key issuance request message received from a mobile terminal, generating an encryption key from data (H(F(VPW))) wherein said value authentication information (F(VPW)) is encoded by a second irreversible calculation process (H) and a master key, generating said electronic key with the use of said value authentication information (F(VPW)) and said generated encryption key, and transmits **[[it]]** said encryption key to said mobile terminal,

in authentication of said electronic key, an authentication function of said electronic key generating a random number (R) and transmitting **[[it]]** said random number to said mobile terminal, receiving authentication information (G(R,F(VPW'))) and said electronic key from said mobile terminal, decrypting code of encrypted part of said electronic key, and validating said electronic key, further extracting said value authentication information (F(VPW)) from said electronic key, generating said authentication information (G(R,F(VPW))) wherein value authentication information (F(VPW)) and said random number (R) are concatenated and encoded by a third irreversible calculation process (G), and collating received authentication information (G(R,F(VPW'))) with generated authentication information (G(R,F(VPW))), verifying that they are identical, thereby authenticating said user.

32. (currently amended) The lock apparatus of claim 31 wherein:

in issuance of said electronic key, generating a second random number (R0), transmitting [[it]] said second random number to said mobile terminal, extracting user identification information (J(LN',R0)) wherein lock number (LN') input to a mobile phone by user and said second random number (R0) are concatenated and encoded by a fourth irreversible calculation process (J) from said electronic key issuance request message received from said mobile terminal, generating user identification information (J(LN,R0)) wherein lock number (LN) and said second random number (R0) are concatenated and encoded by [[a]] said fourth irreversible calculation process (J), collating received user identification information (J(LN',R0)) with generated user identification information (J(LN,R0)), verifying that they are identical, and authenticating said user, thereby issuing [[an]] said electronic key.

33. (currently amended) The lock apparatus of claim 31 or 32 wherein:

having storage means storing key ID of said issued electronic key,

in authentication of said electronic key, collating received key ID of said electronic key with said key ID stored in said storage means,

executing authentication process based on said authentication information (G(R,F(VPW'))) received from said mobile terminal and said electronic key.

Claims 34-39 – (canceled)